

### REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-27 remain active in this case, Claims 1, 6, 10, 14, 18, 26 and 27 having been amended, and Claim 4 canceled by the present amendment.

In the outstanding Office Action, Claims 1-27 were rejected under 35 U.S.C. §102(e) as being anticipated by Hurst et al. (USP 7,200,867, hereinafter "Hurst").

In light of the outstanding ground for rejection, the independent Claims 1, 6, 10, 14, 18, 26, and 27 have been amended to clarify the claimed invention, and thereby more clearly patentably define over the cited prior art. To that end, independent Claims 1, 6, 10, 14, 18, 26, and 27 have been amended to include the subject matter of Claim 4, which has been canceled. No new matter has been added.

Briefly recapitulating, Applicants' relates to a technique for preventing a cookie leakage which would occur due to cross-site scripting vulnerability, and analyzes a script which is assumed to transfer a cookie, when receiving it from a server. In order to prevent illegal transmission of information such as a cookie, when a script is executed, a transfer destination is checked, and collated with a permitted transfer list.

Hurst at col. 4, lines 10-67 describes "the system determines if the links to the pages are checked to determine if the transfer of the page is safe or not." However, although Hurst discloses "security vulnerability," Hurst does not pay attention to a leakage of a cookie or other information. That is, Hurst does not disclose processing for determining whether a cookie is permitted to be transmitted or not.

The system of Hurst is a system of a client, whereas that of the present invention, stated in independent Claims 1, 6, 12, 16, and 18, is a system of a communication gateway apparatus to be coupled between a server and a client.

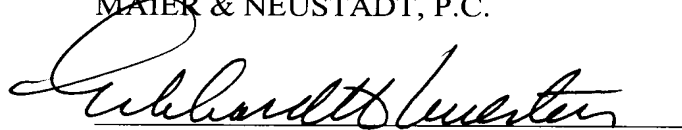
Furthermore, as per the Hurst disclosure, the Hurst system obtains a typical access to a server in advance to form a "permission list,"<sup>1</sup> and then obtains a nontypical access to check whether a link not indicated in the permission list is established or not. On the other hand, in Applicants' invention, a manager sets a permission list in advance to inhibit, in an actual environment, transmission to the client of a Web page where a link not indicated by the permission list may be established.

It is respectfully submitted that Hurst does not disclose paying attention to a leakage of the information transmitted from the server through the client. Accordingly, it is respectfully submitted that Hurst fails to obviate the claimed invention and that the outstanding rejection based on Hurst has been overcome. Withdrawal thereof is respectfully requested.

Consequently, in view of the present amendment and in light of the above comments, no further issues are believed to be outstanding, and the present application is believed to be in condition for allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,  
MAYER & NEUSTADT, P.C.



Eckhard H. Kuesters  
Attorney of Record  
Registration No. 28,870

Customer Number  
**22850**

Tel: (703) 413-3000  
Fax: (703) 413 -2220  
(OSMMN 08/07)

---

<sup>1</sup> Hurst, column 6, lines 58-67, "Then, in a step 230, the Internet security analysis system 100 checks a predetermined--but extensible--list of known, common security vulnerabilities. Typically, these security vulnerabilities are "exploits" which have become well known to security experts. The Internet security analysis system scans the target Web site to determine whether or not any of the exploits are present at the target Web site."